❒ Original

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
Information associated with Apple DSID 10701543533 that is stored at premises controlled by Apple, Inc., more fully described in Attachment A

Case No. 24-M-332 (SCD)

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Northern District of California
(identify the person or describe the property to be searched and give its location):

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before 2-23-24 *(not to exceed 14 days)*

❒ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Hon. Stephen C. Dries.
(United States Magistrate Judge)

❒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

❒ for _____ days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of _____.

Date and time issued: 2-9-24. 10;25 am

Stephen C. Dries
Judge's signature

City and state: Milwaukee, Wisconsin

Hon. Stephen C. Dries, United States Magistrate Judge
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with **johnsonquandale@icloud.com, DSID 10701543533**, that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at One Apple Park Way, Cupertino, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple Inc. ("Apple")

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Apple, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on or about August 14, 2023, and extended on or about November 13, 2023, Apple is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile

Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and

bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and capability query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My and AirTag logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with AirTags, Location Services, Find My, and Apple Maps;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of 18 U.S.C. §§ 1028(a)(7) (possession of means of identification in connection with another felony offense, including wire fraud); 1029(a)(2) (use and trafficking of access devices); 1029(a)(3) (possession of 15 or more access devices); and 1343 (wire fraud), those violations involving QuanDale T. JOHNSON and occurring after October 1, 2019, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. Records and information relating to access, use, possession, sale, or control over stolen personal information, financial information, access devices, and/or electronic devices;

b. Records and information relating to digital marketplaces;

c. Records and information relating to malicious software;

d. Records and information relating to finances and financial transactions, including financial institutions and financial instruments;

e. Records and information relating to virtual currency, such as bitcoin, virtual currency accounts, and virtual currency transfers;

f. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

g. Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

h. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

i. The identity of the person(s) who communicated with the user ID about matters relating to identify theft, access device fraud, or wire fraud, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Information associated with Apple DSID 10701543533 that is stored at premises controlled by Apple, Inc., more fully described in Attachment A

Case No. 24-M-332 (SCD)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attahcment A.

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 1028(a)(7), 1029 (a)(2), 1029(a)(3), and 1343.	Identity Theft, Access Device Fraud, Wire Fraud

The application is based on these facts:

See attached affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

FBI Special Agent Domnall Hegarty
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by Telephone *(specify reliable electronic means)*.

Date: 2-9-24

Judge's signature

City and state: Milwaukee, Wisconsin

Hon. Stephen C. Dries, United States Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Domnall Hegarty, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that stored at premises owned, maintained, controlled, or operated by Apple Inc. ("Apple"), an electronic communications service and/or remote computing service provider headquartered at One Apple Park Way, Cupertino, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I have been a Special Agent with the Federal Bureau of Investigation since October 2022. I am currently assigned to the FBI Milwaukee Division's Cyber Crime Task Force. As a Special Agent for the FBI, I conduct investigations of criminal computer intrusion matters involving botnets, illicit online marketplaces, the use of malware, and other computer-based fraud, as well as national security matters. I was a Computer Scientist with the FBI from 2018 until I became a Special Agent in 2022. As an FBI Computer Scientist, I provided technical analysis support to Special Agents working on cyber investigations.

3. This affidavit is based upon information supplied to me by other law enforcement officers, including other special agents employed by the FBI. It is also based upon my personal involvement in this investigation and on my training and experience. In submitting this affidavit, I have not included every fact known to me about the investigation, but instead have included only those facts that I believe are sufficient to establish probable cause to support this seizure warrant application.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 1028(a)(7) (possession of means of identification in connection with another felony offense, including wire fraud); 1029(a)(2) (use and trafficking of access devices); 1029(a)(3) (possession of 15 or more access devices); and 1343 (wire fraud) have been committed by QuanDale T. JOHNSON (born XX/XX/1998). There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, and/or fruits of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

6. On March 22, 2023, I and other FBI agents executed a warrant (the "Premises Warrant") to search the person of QuanDale T. JOHNSON (born XX/XX/1998) and the premises at 2942 N 2nd Street #202, Milwaukee, Wisconsin 53212

(the "Premises"). The search warrant had been issued on March 17, 2023, by the Honorable Stephen C. Dries, United States Magistrate Judge, under Case No. 23-M-340 (SCD). The warrant was supported by an affidavit (the "Premises Affidavit") setting forth probable cause for the search. In brief summary, law enforcement had determined that JOHNSON was a customer of an illicit online marketplace named Genesis Market, which compiled stolen data from malware-infected computers around the globe and packaged it for sale.

7. As further described in the Premises Affidavit, the FBI found that a Genesis Market account under the username "robinkingg" had been funded through virtual currency deposits in the form of Bitcoin. Records obtained from the cryptocurrency exchange Coinbase showed that these deposits flowed from an account belonging to JOHNSON, with registration email johnsonquandale@icloud.com. This address is hosted by Apple and associated with Apple's iCloud cloud storage and cloud computing service, described further below.

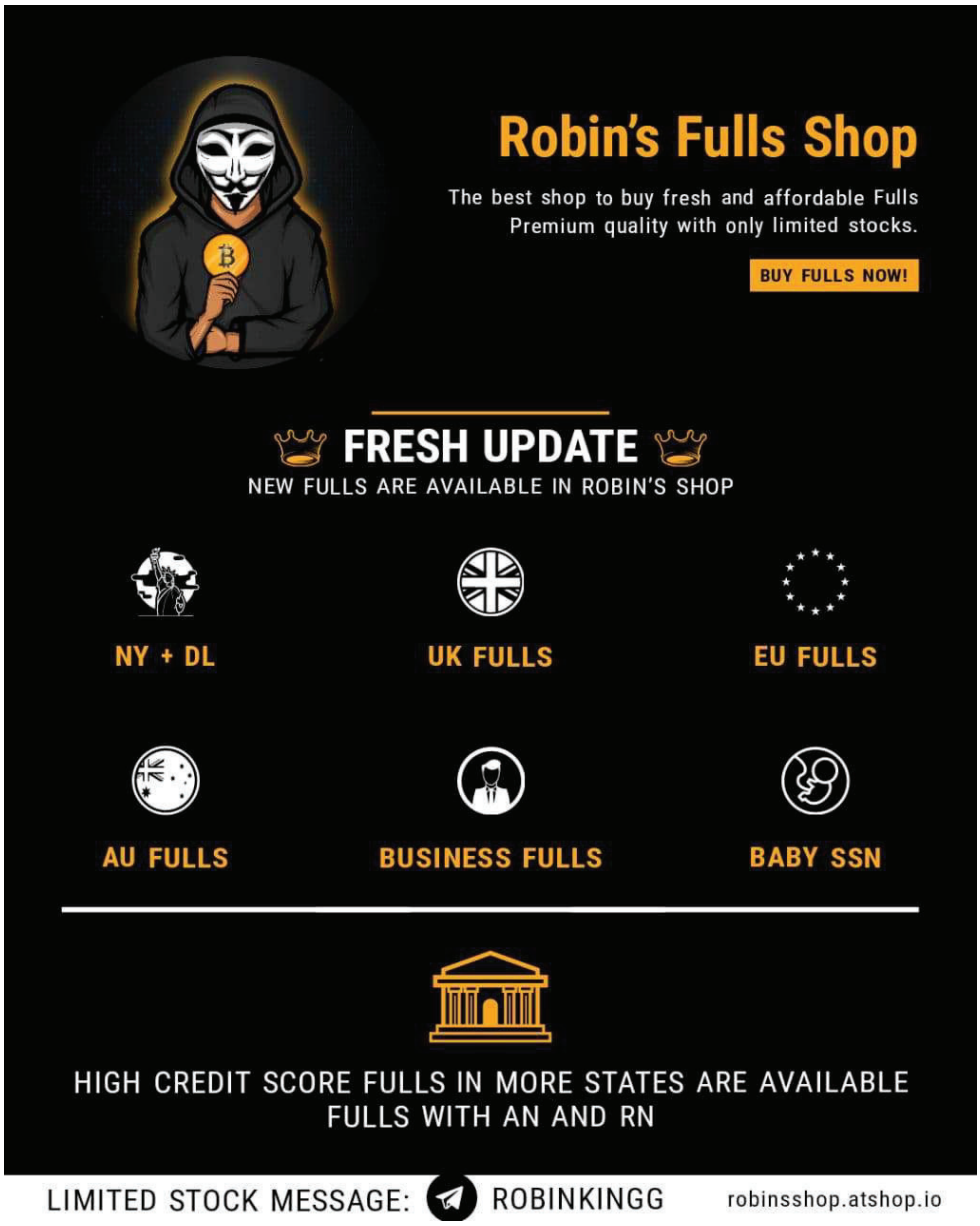
8. In executing the Premises Warrant, the FBI seized multiple laptop computers and smartphones. This included two Apple iPhones that were seized from the Premises, and a third iPhone seized from JOHNSON's person.

9. The FBI's review of the various devices seized further linked JOHNSON to Genesis Market user "Robinkingg." One of the seized laptops contained saved login credentials for "'genesis.market" (a domain that Genesis Market used prior to its seizure by federal law enforcement in April 2023) with the username "Robinkingg." Web browsing history identified on this same device showed numerous logins to Genesis Market, and also reflected browsing to unique packages of stolen credentials purchased by "Robinkingg." JOHNSON's browsing history also indicated instances of logins to various websites using

stolen credentials JOHNSON obtained from Genesis Market using the "Robinkingg" account.

10. JOHNSON's devices also contain evidence of other activities. For example, the FBI found documents containing personal identifying information for approximately 147 individuals, to include various combinations of names, dates of birth, addresses, phone numbers, and Social Security numbers. JOHNSON also possessed bank account credentials and/or credit card numbers for a subset of these individuals. The FBI is not aware of any legitimate reason for JOHNSON's possession of this information. Over 150,000 additional username and password combinations were identified within his devices. The FBI also located screenshots depicting online bank account pages that displayed names of individuals apparently unrelated to JOHNSON.

11. The FBI's review of JOHNSON's devices located graphics for a "Robinsshop," hosted at robinsshop.atshop.io. "Robinsshop" appeared to advertise "fulls" for sale from multiple locations, to include the United Kingdom, Australia, and the European Union. Based on my training and experience, "fulls" can refer to "full identities," often including personally identifiable information, Driver's Licenses or other forms of identification, and/or online financial accounts. At least one graphic contained the text "ROBINKINGG" next to a logo for the encrypted instant messaging service Telegram. (As mentioned above, "Robinkingg" was also the username for JOHNSON's Genesis Market account.)



(An example of a "robinsshop" graphic found on a laptop seized from the PREMISES)

12. Investigators also recovered a screenshot displaying an administration page at the robinsshop.atshop.io address. The screenshot appeared to show the creation of a new product listing called "California+."[1]

13. Records obtained from Apple in March 2023 confirmed that the Apple ID johnsonquandale@icloud.com was registered to QuanDale Johnson. The account was linked to two phone numbers and an address, all of which were previously associated with additional accounts attributed to JOHNSON. The unique identifier, or DSID, associated with this account is 10701543533.

14. A blue iPhone 12 Pro Max seized from the Premises during the execution of the Premises Warrant was also associated with Apple ID johnsonquandale@icloud.com. Snapchat conversations stored on this device and reviewed by the FBI included references by JOHNSON to Genesis Market and JOHNSON's control of the Telegram account "@Robinkingg." JOHNSON also discussed acquiring fake identification documents to make fraudulent Western Union withdrawals, generating fraudulent checks, utilizing CPNs[2] to purchase tradelines,[3] acquiring Paycheck Protection Program loans, and conducting SIM

[1] Atshop.io is marketed as a place for vendors to sell various digital merchandise. Investigators first browsed robinsshop.atshop.io in approximately October 2023. At that time, the page indicated that "Robinsshop" was no longer active because the administrator had allowed the subscription to expire.

[2] A CPN, or Credit Profile Number, is a term used market a stolen or unused Social Security Number as a way for individuals with poor credit history to establish a new credit identity.

[3] A tradeline is a record of activity for any type of credit reported to a credit reporting agency. Tradelines can be purchased to add an additional user to an existing line of credit owned by another individual. This enables individuals to "inherit" the credit history of the existing credit card account holder, and makes it easier to obtain multiple new credit card accounts and higher credit limits.

swapping,[4] among other activities. However, activity on this phone appears to cease after approximately October 2022. A different iPhone was seized from JOHNSON's person during the execution of the Premises Warrant, but the FBI has not yet gained access to this device. Based on my training and experience, smartphone users often migrate accounts and other data when switching or upgrading devices.

15. Records provided by Coinbase in January 2023, Venmo in March 2023, Landmark Credit Union in March 2023, and Paypal in February 2023, all list johnsonquandale@icloud.com as an email address associated with JOHNSON's accounts. Online services of this kind often send email confirmations or receipts of transactions to the email address on file for the account.

16. Records supplied by Apple in March 2023 also indicate that JOHNSON had enabled the following features for the iCloud account associated with johnsonquandale@icloud.com: iCloud backup, Bookmarks, Calendar, iCloud Photos, Contacts, Find My Friends, iCloud Drive, iCloud reminders, Mail, Mail Header, and Notes. However, iMessage backups were not enabled. The account type was designated "iCloud+," indicating a paid version of iCloud that allows for additional cloud storage space. Certain messaging applications (such as Snapchat and Whatsapp) allow the user to store a backup of conversations in iCloud.

---

[4] SIM Swapping is a method of assigning a new mobile device to an existing phone number without the permission of the account owner, enabling the new device owner to receive all phone calls and messages sent to the original number. This is often used to gain access to two factor authentication codes sent via SMS, enabling fraudulent access to bank and financial accounts.

BACKGROUND CONCERNING APPLE[5]

17. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

18. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct audio and video calls.

c. iCloud is a cloud storage and cloud computing service from Apple that allows its users to interact with Apple's servers to utilize iCloud-connected services to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any

---

[5] The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf; "Manage and use your Apple ID," available at https://support.apple.com/en-us/HT203993; "iCloud," available at http://www.apple.com/icloud/; "Introduction to iCloud," available at https://support.apple.com/kb/PH26502; "What does iCloud back up?," available at https://support.apple.com/kb/PH12519; and "Apple Platform Security," available at https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf.

Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on iCloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iCloud Backup allows users to create a backup of their device data. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

d. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

e. Find My allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of iOS devices, as well as share their location with other iOS users. It also allows owners of Apple devices to manage, interact with, and locate AirTags, which are tracking devices sold by Apple.

f. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

g. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or

through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

19. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. The account identifier for an Apple ID is an email address, provided by the user. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

20. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive

or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

21. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "capability query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the "Find My" service, including connection logs and requests to remotely find, lock, or erase a device, are also maintained by Apple.

22. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer

service, including communications regarding a particular Apple device or service, and the repair history for a device.

23. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Some of this data is stored on Apple's servers in an encrypted form but may nonetheless be decrypted by Apple. As noted above, records and data associated with third-party apps, including the instant messaging service WhatsApp and Snapchat, may also be stored on iCloud.

24. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

25. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, and as discussed above, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

26. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

27. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. JOHNSON moved significant amounts of cryptocurrency through his Coinbase account. The blue iPhone 12 Pro Max discussed above contained conversations regarding the use of CashApp, Zelle, and Venmo to move and withdraw money. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

28. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes

under investigation including information that can be used to identify the account's user or users.

CONCLUSION

29. Based on the forgoing, I request that the Court issue the proposed search warrant.

30. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with **johnsonquandale@icloud.com, DSID 10701543533**, that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at One Apple Park Way, Cupertino, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple Inc. ("Apple")

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Apple, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on or about August 14, 2023, and extended on or about November 13, 2023, Apple is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile

Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and

bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and capability query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My and AirTag logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with AirTags, Location Services, Find My, and Apple Maps;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of 18 U.S.C. §§ 1028(a)(7) (possession of means of identification in connection with another felony offense, including wire fraud); 1029(a)(2) (use and trafficking of access devices); 1029(a)(3) (possession of 15 or more access devices); and 1343 (wire fraud), those violations involving QuanDale T. JOHNSON and occurring after October 1, 2019, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. Records and information relating to access, use, possession, sale, or control over stolen personal information, financial information, access devices, and/or electronic devices;

b. Records and information relating to digital marketplaces;

c. Records and information relating to malicious software;

d. Records and information relating to finances and financial transactions, including financial institutions and financial instruments;

e. Records and information relating to virtual currency, such as bitcoin, virtual currency accounts, and virtual currency transfers;

f. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

g. Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

h. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

i. The identity of the person(s) who communicated with the user ID about matters relating to identify theft, access device fraud, or wire fraud, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.